



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/918,742      | 07/31/2001  | Ernst-Michael Hamann | DE920000056US1      | 2722             |

7590 01/25/2005

Jeanine S. Ray-Yarletts  
IBM Corporation  
T81/503  
PO Box 12195  
Research Triangle Park, NC 27709

EXAMINER

SCHUBERT, KEVIN R

ART UNIT PAPER NUMBER

2137

DATE MAILED: 01/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/918,742

Applicant(s)

HAMANN ET AL.

Examiner

Kevin Schubert

Art Unit

2137

– The MAILING DATE of this communication appears on the cover sheet with the correspondence address –  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 31 July 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-16 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 31 July 2001 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

### DETAILED ACTION

Claims 1-16 have been considered. The examiner suggests that minor spelling and grammar errors be corrected in the Specification.

5

#### *Drawings*

The drawings are objected to because of the following minor informalities: "EPROM" in Fig 1 should be "EEPROM" as referenced in the application (Page 6, 4<sup>th</sup> paragraph). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

20

#### *Claim Objections*

Claims 2 and 3 are objected to because of the following informalities: the phrase "at least following" should be replaced with the phrase "at least the following". Appropriate correction is required.

25

Claim 6 is objected to because of the following informalities: the word "seurity" is a misspelled version of "security". Appropriate correction is required.

Art Unit: 2137

***Claim Rejections - 35 USC § 112***

Claims 14-16 are rejected under 35 U.S.C 112, 5<sup>th</sup> paragraph as being multi-dependent claims.

The claims have been withdrawn from consideration.

5

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

10

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

15

Claims 1-4,6-11, and 13-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Geiger, U.S. Patent No. 6,463,534.

20

As per claim 1, the applicant describes a security token with the following limitations which are met by Geiger:

a) a Random Access Memory (RAM) (Col 11, lines 65-67);

b) an Electrical Erasable Programmable Read Only Memory (EEPROM) (Col 11, lines 65-67; Col

25 4, lines 62-64; Col 17, lines 18-19);

c) One or more Microprocessors (Col 11, lines 65-67);

d) a Read Only Memory (Col 11, lines 65-67; Col 4, lines 61-62);

e) And characterized in that said EEPROM having at least an object containing a user certificate and an object containing a certificate of the certification authority (CA) of said user certificate (root

30 certificate), wherein said root certificate is being write protected, and a verification component for

Art Unit: 2137

checking authentication of said user certificate using information of said root certificate (Col 5, lines 3-10; Col 4, lines 62-64);

5 The applicant describes a method for the secure usage and importation of digital certificates based on the idea that a security token should import or be pre-loaded with a root certificate to facilitate verification of imported user certificates since, according to the applicant, "the usage of key and certificate objects stored in the token cannot be guaranteed without a valid root certificate of the CA...[and] the root certificate may only be retrieved from an external database" (pages 2-3). The applicant also discloses that the "security token may be used in connection with any portable data processing device, e.g. personal digital assistant or mobile phone [and] a smart card may be used as a preferred embodiment" (page 5).

10 Geiger discloses a method of verifying imported digital certificates through a smart card in a mobile phone (Fig 4) which revolves around the idea of pre-loading a wireless client device, which may be a smart card (Col 13, lines 15-16; Col 11, lines 65-67), with a root public key certificate for verification purposes.

15 Regarding parts a) through d), the use of a smart card satisfies all the limitations of RAM, EEPROM, a microprocessor, and ROM because a typical smart card has all these features. The applicant should note that Fig 1 (of applicant's Drawings) illustrates that a typical smart card has all these features. The applicant should also note that Geiger does reference that the security token, or smart card, has EEPROM and ROM as referenced by the lines above.

20 Regarding part e), the applicant should note that the EEPROM (Col 4, lines 62-64) stores a user certificate and an object of the certification authority (Col 5, lines 3-10). Also, Geiger discloses that the keys and certificates are stored on the security token, or smart card, if a smart card is used as it is in the preferred embodiment (Col 17, lines 18-19). If a smart card is not used, the keys and certificates are stored on whichever token is being used. Lastly as for the part about the root certificate being write  
25 protected, Geiger discloses that once written "access to the certificate storage area must be restricted" (Col 4, lines 63-64).

Art Unit: 2137

As per claim 2, the applicant describes a security token according to claim 1, which is met by Geiger (see above), with the following limitations which are also met by Geiger:

Wherein said user certificate comprises at least the following information:

- a) a name of issuer (Col 3, lines 24-27);
- 5 b) an identifier (ID) of said issuer (Col 3, lines 24-27);
- c) a user identifier (ID) (Col 3, lines 24-27);
- d) a HASH algorithm (Col 4, line 5);
- e) a signature algorithm (Col 3, lines 24-27);
- f) a public key (Col 3, line 27);
- 10 g) a digital signature (Col 3, lines 24-27);

A typical phone is installed with a smart card which contains the phone's own public key certificate plus the CA's public key certificate (Col 5, lines 3-4). As describes by Geiger, a typical public key certificate contains the name of an issuer (CA), an identifier of said issuer (digital signature of CA), a user identifier (serial number), a hash algorithm (hash), a signature algorithm (digital signature of CA), a public key (public key certificate), and a digital signature (digital signature of CA).

As per claim 3, the applicant describes the security token of claim 1, which is met by Geiger (see above), with the following limitations which are also met by Geiger:

Wherein said root certificate comprises at least following information:

- 20 a) a certification authority name (Col 5, lines 3-6);
- b) a certification authority identification (ID) (Col 5, lines 3-6);
- c) a HASH algorithm (Col 4, lines 10-21);
- d) a signature algorithm (Col 5, lines 3-6);
- e) a public root key (Col 5, lines 3-6);
- 25 f) a digital signature (Col 5, lines 3-6);

Art Unit: 2137

As per claim 4, the applicant describes the security token of claim 1, which is met by Geiger (see above), with the following limitations which are also met by Geiger:

- a) a public root key (Col 6, lines 1-4);
- b) a user's public key (Col 6, lines 1-4; Col 9, lines 43-45);
- 5 c) a user's private key (Col 6, lines 1-4; Col 9, lines 43-45);

The applicant should note that the certificates are stored in the EEPROM of the smart card (Col 4, lines 62-64; Col 17, lines 18-19).

10 As per claim 6, the applicant describes the security token of claim 1, which is met by Geiger (see above), with the following limitation which is also met by Geiger:

Wherein said security token is a smart card (Col 11, lines 64-67);

As per claim 7, the applicant describes a method for initializing a security token comprising the following steps:

- 15 a) transferring a root certificate of a certification authority into said security token using a secure transmission environment (Col 5, lines 3-10);
- b) securing the root certificate against modifications (Col 5, lines 3-10);
- c) storing a verification component into said security token allowing use or replacement of a user certificate only when said user certificate is authenticated by said root certificate (Col 6, lines 5-25);

20 The lines referenced above describe the verification component of the security token which happens when the phone turns on and the certificates it has saved are verified by the root certificate. The applicant should also note that verification also takes place when a certificate is downloaded (Col 18, lines 52-62). Furthermore, the verification code runs in ROM (Col 4, lines 61-62).

25 As per claim 8, the applicant describes the method of claim 7, which is met by Geiger (see above), with the following limitation which is also met by Geiger:

- d) storing public root key additionally to said root certificate (Col 5, lines 3-5);

As per claim 9, the applicant describes the method of claim 1, which is met by Geiger (see above), with the following limitations which are also met by Geiger:

a) retrieving a public root key from said root certificate (Col 4, line 14);

b) generating a HASH over a user certificate using the HASH algorithm specified in said user certificate (Col 4, line 16);

c) retrieving and decrypting a digital signature contained in said user certificate by applying said public root key resulting in a HASH of said user certificate (Col 4, lines 10-21);

d) allowing use of said user certificate for signing said information with said digital signature when both HASHs are identical (Col 4, lines 10-21).

As per claim 10, the applicant describes the method of claim 9, which is met by Geiger (see above), with the following limitation which is also met by Geiger:

Wherein said information is a document or electronic mail (Col 6, lines 41-43; Fig 4).

As per claim 11, the applicant limits the method of claim 9, which is met by Geiger (see above), with the following limitation which is also met by Geiger:

Wherein said user certificate and said root certificate are sent to said application system and said steps a) – d) are accomplished on said application system (Col 13, lines 26-33).

As per claim 13, the applicant describes a method for replacing a user certificate stored in a security token according to claim 1, which is met by Geiger (see above), with the following limitations which are also met by Geiger:

a) receiving a new user certificate from the certification authority and storing it into said EEPROM of said security token as a temporary object (Col 1, lines 33-48);

b) generating a HASH over a new user certificate using a HASH algorithm specified in said new user certificate (Col 4, lines 10-21);



Art Unit: 2137

c) retrieving a digital signature contained in said new user certificate and decrypting said digital signature by applying a public root key retrieved from a root certificate resulting in a HASH of said user certificate (Col 4, lines 10-21);

d) permanently storing said new user certificate when both HASHs are identical (Col 4, lines 10-21);

The attribute authority, which delivers a digital certificate to the wireless client device, such as a mobile phone, is the certificate authority. The use of the EEPROM of the smart card is disclosed by Geiger (Col 4, lines 62-64; Col 17, lines 18-19).

Regarding parts b) and c), the section referenced by (Col 4, lines 10-21) illustrates how the stored root certificate is used to validate that an incoming certificate is authentic.

As per claim 14, the applicant describes the following which is anticipated by Geiger:

Client-Server system having a client with a security token according to claim 1 to 6 (Col 13, lines 15-17);

As per claim 15, the applicant describes the following which is anticipated by Geiger:

Data processing system using a security token according to claim 1 to 6 (Col 11, lines 64-67; Fig 4);

The data processing system is the mobile phone which uses the security token, or smart card.

As per claim 16, the applicant describes the following which is anticipated by Geiger:

Computer program product stored on a computer-readable media containing software for performing of the method according to claims 7 to 13 (Col 11, lines 64-67; Col 12, lines 1-8);

The computer program product and software are instructions and the computer-readable media is the smart card.

Art Unit: 2137

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 5 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Geiger.

As per claim 5, the applicant describes the security token according to claim 1, which is met by Geiger (see above), with the following limitation which is also anticipated by Geiger:

Wherein said verification component is part of the operating system of said security token (Col 4, lines 61-62);

As illustrated by the applicant in the Drawings, the Operating System is housed in the ROM of the smart card. Geiger describes a system where verification code is stored in ROM (Col 4, lines 61-62). Though not explicitly stated, the ROM Geiger is referring to is that of the smart card where the certificate storage and authentication take place. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to make the verification component a part of the operating system of the smart card.

As per claim 12, the applicant describes the method of claim 9, which is met by Geiger (see above), with the following limitation which is also met by Geiger:

Checking the validity of the root certificate before retrieving said public root key (Col 5, lines 3-10);

Geiger describes all the limitations of claim 9. However, Geiger fails to disclose checking the validity of the root certificate when the public root key is retrieved because in Geiger's system the root certificate is transferred in a secure environment (Col 5, lines 3-10) and there is no reason to believe that the root certificate could be tampered with. It would have been obvious to one of ordinary skill in the art

Art Unit: 2137

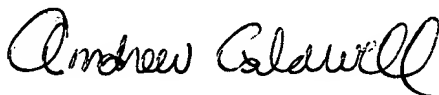
at the time the invention was filed to incorporate checking the validity of the root certificate before retrieving the public root key in a system where the root certificate could be compromised.

5 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where  
10 this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should  
15 you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

\*\*\*

  
**ANDREW CALDWELL**  
**SUPERVISORY PATENT EXAMINER**

20

25